#10

10/3/3

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Application

Applicant(s):	Mayer et al.
Case:	6-9-1
Serial No.:	09/483,876
Filing Date:	January 18, 2000
Group:	2141
Examiner:	Adnan M. Mirza

I hereby certify that this paper is being deposited on this date with the U.S. Postal Service as first class mail addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

Signature: _____ Date: September 17, 2003

Title: Method and Apparatus for Analyzing One or More Firewalls

---

APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Applicants hereby appeal the final rejection dated May 30, 2003, of claims 1 through 29 of the above-identified patent application.

REAL PARTY IN INTEREST

The present application is assigned to Lucent Technologies Inc., as evidenced by an assignment recorded on April 14, 2000 in the United States Patent and Trademark Office at Reel 010705, Frame 0547. The assignee, Lucent Technologies Inc., is the real party in interest.

RELATED APPEALS AND INTERFERENCES

There are no related appeals and interferences.

STATUS OF CLAIMS

Claims 1 through 29 are pending in the above-identified patent application. Claims 1 through 29 remain rejected under 35 U.S.C. §103(a) as being

unpatentable over Reid et al. (United States Patent Number 6,182,226), and further in view of Flint et al. (United States Patent Number 6,453,419).

STATUS OF AMENDMENTS

There have been no amendments filed subsequent to the final rejection.

SUMMARY OF INVENTION

The present invention provides a method (400) and apparatus (200) for analyzing the operation of one or more network gateways (120, 150), such as firewalls or routers, that perform a packet filtering function in a network environment (100). Given a user query (410), the disclosed firewall analysis tool simulates the behavior of the various firewalls, taking into account the topology of the network environment (e.g., page 7, lines 5-14), and determines which portions of the services or machines specified in the original query would manage to reach from the source to the destination (450). The relevant packet-filtering configuration files are collected and an internal representation of the implied security policy is derived.

ISSUES PRESENTED FOR REVIEW

Whether Claims 1-29 are properly rejected under 35 U.S.C. §103(a) as being unpatentable over Reid et al., and further in view of Flint et al.

GROUPING OF CLAIMS

The rejected claims do not stand and fall together. More particularly, for the reasons given below, Applicant believes that each of the dependent claims 6/11/16/24 provide independent bases for patentability apart from the rejected independent claims.

ARGUMENT

Claims 1 through 29 are rejected under 35 U.S.C. §103(a) as being unpatentable over Reid et al., and further in view of Flint et al.

In particular, the Examiner asserts that Reid discloses a method for analyzing at least one gateway in a network. The Examiner further asserts that Reid generates a gateway-zone graph that models said network.

Applicants note that Reid teaches "*a visual means by which access control can be defined* and easily understood through flowchart style diagrams." Col. 7, lines 25-27. Figure 3 is a graphical representation of Access Control Language (ACL) commands. The graphical representation is created by a user to define the access control rules for a given firewall. The graphical representation is then used to generate the access control commands which will be implemented by the firewall. Thus, *the graph is created by the user to input rules to the firewall.*

Flint et al. was also cited by the Examiner in rejecting claims 1 through 29 for its disclosure that Flint discloses "the regions that the service bridge, and the access control decisions."

Applicants note that Flint is similar to Reid and also teaches a graphical user interface for conveniently defining rules for a firewall. Again, the flowchart is created by the user to define the access control rules. The flowchart is then used to generate the access control commands which will be implemented by the firewall. Thus, *the graph is created by the user to input rules to the firewall.*

Independent claims 1, 12, 19, and 27 require generating a gateway-zone graph that models said network *based on said packet filtering configuration file.* Similarly, independent claims 9 and 28-29 require generating a gateway-zone graph that models said network *based on said packet-filtering rule-base.* Both Reid and Flint use a graphical model to generate rules for a given firewall. The present invention, on the other hand, generates the graphical model from the rules of one or more firewalls.

Conclusion

Thus, Reid or Flint (alone or in combination) do not disclose or suggest generating or analyzing a "gateway-zone graph that models said network based on said packet filtering configuration file," as required by independent claims 1, 12, 19, and 27 and do not disclose or suggest generating a "gateway-zone graph that models said network based on said packet-filtering rule-base," as required by independent claims 9

and 28-29.

The rejections of the independent claims under section §103 in view of Reid et al. or Flint et al., alone or in any combination, are therefore believed to be improper and should be withdrawn.

Dependent Claims

Claims 6, 11, 16, and 24 specify a limitation providing additional bases for patentability. Specifically, the Examiner rejected claims 6, 11, 16, and 24 under 35 U.S.C. §103(a) as being unpatentable over Reid et al., and further in view of Flint et al. Claims 6 and 24 require "the step of transforming said packet filtering configuration files into a table of logical rules that are processed during said evaluating step." Claim 11 requires "the step of transforming said packet-filtering rule-base into a table of logical rules." Claim 16 requires "wherein said packet filtering configuration files are expressed as a set of logical rules." The Examiner asserts that Reid discloses further comprising the step of transforming said packet filtering configuration files into a table of logical rules that are processed during said evaluating step (col. 7, lines 33-39).

As previously noted, Reid is directed to defining access control rules. Reid, in the text cited by the Examiner, teaches that "access control rules can be *defined* with flexibility previously unknown in the industry." Col. 7, lines 33-34. Reid does not address the step of evaluating queries and does not disclose the step of transforming packet filtering configuration files into a table of logical rules that are processed during said evaluating step.

Thus, Reid et al. or Flint et al., alone or in combination, do not disclose or suggest "the step of transforming said packet filtering configuration files into a table of logical rules that are processed during said evaluating step," as required by claims 6 and 24, do not disclose or suggest "the step of transforming said packet-filtering rule-base into a table of logical rules," as required by claim 11, and do not disclose or suggest "the step of transforming said packet filtering configuration files into a table of logical rules that are processed during said evaluating step," as required by claim 24.

The remaining rejected dependent claims are believed allowable for at least the reasons identified above with respect to the independent claims.

The attention of the Examiner and the Appeal Board to this matter is appreciated.

Respectfully,

Date: September 17, 2003

Kevin M. Mason
Attorney for Applicant(s)
Reg. No. 36,597
Ryan, Mason & Lewis, LLP
1300 Post Road, Suite 205
Fairfield, CT 06824
(203) 255-6560

APPENDIX

1. A method for analyzing at least one gateway in a network, said at least one gateway having a packet filtering configuration file including a plurality of rules, said network having a plurality of addresses, said method comprising the steps of:

generating a gateway-zone graph that models said network based on said packet filtering configuration file, said gateway-zone graph having at least one gateway node corresponding to said at least one gateway and at least two zone nodes, wherein said at least one gateway is a packet filtering machine and each of said zone nodes correspond to a partitioned collection of said addresses created by said at least one gateway;

receiving a query inquiring whether one or more given services are permitted between at least one source address and at least one destination address; and

evaluating said query against each of said rules associated with each gateway node in said gateway-zone graph that is encountered between said at least one source address and said at least one destination address.

2. The method of claim 1, wherein said rules are expressed as rule-base objects.

3. The method of claim 1, wherein said gateway-zone graph is derived from a network topology file.

4. The method of claim 1, wherein said query includes a wildcard for at least one of said service, source address or destination address.

5. The method of claim 1, further comprising the step of determining a portion of said one or more given services that are permitted between at least one source address and at least one destination address.

6. The method of claim 1, further comprising the step of transforming said packet filtering configuration files into a table of logical rules that are processed

during said evaluating step.

7. The method of claim 1, wherein said query consists of a source host-group, a destination host-group, and a service host-group.

8. The method of claim 1, wherein said query specifies a location where packets are to be inserted into the network that is different from a source address.

9. A method of modeling a network having a plurality of gateway devices, comprising the steps of:

identifying each gateway device in said network having a packet-filtering rule-base and each zone in said network defined by said gateway devices; and

generating a gateway-zone graph that models said network based on said packet-filtering rule-base, said gateway-zone graph having a gateway node corresponding to each of said gateway devices and a zone node corresponding to each of said zones.

10. The method of claim 9, wherein said gateway-zone graph is derived from a network topology file.

11. The method of claim 9, further comprising the step of transforming said packet-filtering rule-base into a table of logical rules.

12. An apparatus for analyzing at least one gateway in a network, said at least one gateway having a packet filtering configuration file including a plurality of packet filtering rules, said network having a plurality of addresses, said tool comprising:

a user interface for receiving a query inquiring whether one or more given services are permitted between at least one source address and at least one destination address, wherein each of said source addresses and said destination addresses correspond to one of said zones; and

a user interface for indicating a portion of said one or more given services that are permitted between a portion of said at least one source address and a portion of

said at least one destination address, said portions obtained by analyzing a gateway-zone graph that models said network based on said packet filtering configuration file with at least one gateway node corresponding to said at least one gateway and at least two zone nodes, wherein each of said zone nodes correspond to a partitioned collection of said addresses created by said at least one gateway.

13. The method of claim 12, wherein said rules are expressed as rule-base objects

14. The method of claim 12, wherein said gateway-zone graph is derived from a network topology file.

15. The method of claim 12, wherein said query includes a wildcard for at least one of said service, source address or destination address.

16. The method of claim 12, wherein said packet filtering configuration files are expressed as a set of logical rules.

17. The method of claim 12, wherein said query consists of a source host-group, a destination host-group, and a service host-group.

18. The method of claim 12, wherein said user interface allows a user to specify a location where packets are to be inserted into the network that is different from a source address.

19. An apparatus for analyzing at least one gateway in a network, said at least one gateway having a packet filtering configuration file including a plurality of rules, said network having a plurality of addresses, said tool comprising:

a memory for storing computer readable code; and

a processor operatively coupled to said memory, said processor configured to:

generate a gateway-zone graph that models said network based on said packet filtering configuration file, said gateway-zone graph having at least one gateway node corresponding to said at least one gateway and at least two zone nodes, wherein said at least one gateway is a packet filtering machine and each of said zone nodes correspond to a partitioned collection of said addresses created by said at least one gateway;

receive a query inquiring whether one or more given services are permitted between at least one source address and at least one destination address; and

evaluate said query against each of said rules associated with each gateway node in said gateway-zone graph that is encountered between said at least one source address and said at least one destination address.

20. The tool of claim 19, wherein said rules are expressed as rule-base objects

21. The tool of claim 19, wherein said gateway-zone graph is derived from a network topology file.

22. The tool of claim 19, wherein said query includes a wildcard for at least one of said service, source address or destination address.

23. The tool of claim 19, further comprising the step of determining a portion of said one or more given services that are permitted between at least one source address and at least one destination address.

24. The tool of claim 19, further comprising the step of transforming said packet filtering configuration files into a table of logical rules that are processed during said evaluating step.

25. The tool of claim 19, wherein said query consists of a source host-group, a destination host-group, and a service host-group.

26. The tool of claim 19, wherein said query specifies a location where packets are to be inserted into the network that is different from a source address.

27. A computer readable medium having computer readable program code means embodied thereon, said computer readable program code means analyzing at least one gateway in a network, said at least one gateway having a packet filtering configuration file including a plurality of rules, said network having a plurality of addresses, said computer readable program code means comprising:

a step to generate a gateway-zone graph that models said network based on said packet filtering configuration file, said gateway-zone graph having at least one gateway node corresponding to said at least one gateway and at least two zone nodes, wherein said at least one gateway is a packet filtering machine and each of said zone nodes correspond to a partitioned collection of said addresses created by said at least one gateway;

a step to receive a query inquiring whether one or more given services are permitted between at least one source address and at least one destination address; and

a step to evaluate said query against each of said rules associated with each gateway node in said gateway-zone graph that is encountered between said at least one source address and said at least one destination address.

28. A system for modeling a network, comprising:

a memory for storing computer readable code; and

a processor operatively coupled to said memory, said processor configured to:

identify each gateway device in said network having a packet-filtering rule-base and each zone in said network defined by said gateway devices; and

generate a gateway-zone graph that models said network based on said packet-filtering rule-base, said gateway-zone graph having a gateway node corresponding to each of said gateway devices and a zone node corresponding to each of said zones.

29. A computer readable medium having computer readable program code means embodied thereon, said computer readable program code means comprising:

a step to identify each gateway device in a network having a packet-filtering rule-base and each zone in said network defined by said gateway devices; and

a step to generate a gateway-zone graph that models said network based on said packet-filtering rule-base, said gateway-zone graph having a gateway node corresponding to each of said gateway devices and a zone node corresponding to each of said zones.